AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A pink iPhone Model A1897, IMEI 358632092187804 (See Attachment A)

Case No. 4:19 MJ 6319 PLC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

A pink iPhone Model A1897, IMEI 358632092187804 (See Attachment A)

located in the EASTERN District of MISSOURI, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 875(d)	Transmitting in Interstate Commerce Threats to Injure the Reputation of a Person with the Intent to Extort Money

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kassandra L. McKenzie, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/26/19

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Kassandra L. McKenzie, being duly sworn, state the following:

1. I am presently employed as a Special Agent by the Federal Bureau of Investigation ("FBI"), and have been so employed for the past four years. I am currently assigned to investigate Violent Crimes for the St. Louis Division of the FBI. I have received training on, and participated in, criminal investigations involving extortion, human trafficking, car jackings, Hobbs Act Robberies, and possession with the intent to distribute and the distribution of controlled substances. Through the course of these investigations, I have been involved in the use of the following techniques: analyzing telephone pen registers and caller identification system data; analyzing data from mobile telephones; and executing search warrants and arrest warrants.

2. This Affidavit is submitted in support of an application for the issuance of a Search Warrant for a pink iPhone Model A1897, IMEI 358632092187804 (hereinafter referred to as **"subject telephone 1"**) which was recovered from the person of Kailynn Moore-Jones, aka "Jasmine Ramirez" (hereinafter referred to as Moore-Jones), following her arrest on August 26, 2019. **Subject telephone 1** is currently in my possession at the FBI office on Market Street, St. Louis City, Missouri.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Moore-Jones has committed violations of Title 18, U.S.C. § 875(d); transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money, and that there is also probable cause to search **subject telephone 1** for evidence of these crimes, as described in Attachment B.

4. The facts alleged in this affidavit come from my own investigation, my training and experience, information obtained by me, other agents and employees of the FBI, my review

of reports and information provided by Money Gram, Wal-Mart, law enforcement officers and witnesses. As this affidavit is submitted for the limited purpose of establishing probable cause to secure a Search Warrant, it does not set forth all of my knowledge regarding this matter.

THE UNDERLYING INVESTIGATION AND PROBABLE CAUSE

5. Victim R.W., a resident of St. Louis County, Missouri, contacted the FBI on August 21, 2019 to report an ongoing extortion. I responded to R.W.'s place of business, also located in St. Louis County, on August 22, 2019. R.W. told me that an individual, later identified as Moore-Jones, using the alias "Jasmine Ramirez", sent a number of text messages, Facebook messages, phone calls, and emails to R.W.'s cellular telephone and social media platforms demanding money lest she publically release video of R.W. and Moore-Jones having sex. R.W. met Moore-Jones approximately on August 6, 2019 through the prostitution website escortbabylon.net. They arranged an assignation for later that day at the Pear Tree Inn St. Louis Airport. During this meeting and without R.W.'s knowledge, Moore-Jones filmed the ensuing sexual encounter with R.W., herself, and another unidentified woman with her cellular telephone.

6. On approximately August 18, 2019, Moore-Jones sent the victim a number of threatening text messages and phone calls in an effort to collect money from the victim. Moore-Jones demanded $15,000 in three $5,000 increments, threatening that if R.W. did not pay, she would send the sex video she filmed to R.W.'s spouse and employer with the goal to ruin his reputation. Moore-Jones made these communications to the victim through telephone calls from multiple phone numbers and social media platforms. R.W. made partial payments of this sum to Moore-Jones by wiring money to her in Arizona through Money Gram.

7. Moore-Jones continued to call the victim's place of employment and posted a pornographic video on R.W.'s Facebook page, his wife's Facebook page, and his employer's page. On August 23, 2019, R.W. called Moore-Jones and asked what else she wanted. This conversation was consensually monitored and witnessed by FBI Special Agents. Moore-Jones demanded more money and agreed to delete the video from her telephone once she received the money.

8. I conducted searches in law enforcement databases as well as social media pages and found a true name Facebook account for "Kailynn Moore-Jones" [Facebook ID 100025274438252] and a second account for "Kailynn Moore-Jones" [Facebook ID 100015583419233], both having photos which matched the official photos of Moore-Jones.

9. Money Gram provided FBI Special Agents transaction information which revealed that two of the transactions R.W. sent to Moore-Jones on August 18, 2019 were received at a Walmart store located at 455 East Whetmore Road, Tucson, Arizona, which is located in the District of Arizona. I reviewed surveillance footage of these transaction showing Moore-Jones and an unidentified woman picking up the money both times. Each time, Moore-Jones was shown in the surveillance video using an iPhone with a white stripe on the top and bottom of the face with a glittery case, consistent with the description of **subject telephone 1**, while retrieving the money transaction. Through investigation and witness interviews, I know that she was communicating to R.W. while picking up the money. Thus, the threatening messages R.W. received on that day in the Eastern District of Missouri traveled in interstate commerce.

10. On August 26, 2019, Moore-Jones demanded R.W. send Moore-Jones $2,500 through Money Gram. Under the direction and control of law enforcement, R.W. pretended to do so and told Moore-Jones she could retrieve the money. FBI Special Agents observed Moore-Jones exit a white Mercedes-Benz and walk into the Walmart store located at 455 East Whetmore Road,

Tucson, Arizona. Pursuant to a criminal complaint issued by a Magistrate Judge in the Eastern District of Missouri, FBI Special Agents arrested Moore-Jones as she was waiting for the payment from R.W. at the Money Gram business located inside the Walmart store. Moore-Jones called R.W. using **subject telephone 1** while waiting for the transaction to take place but the call ended upon her arrest. **Subject telephone 1** was seized at this time. Immediately following the arrest, Moore-Jones uttered "oh, this is how he wants to do this? I did have sex with him and I have a video," or words to that effect.

11. On September 4, 2019, FBI Agents served a federal search warrant issued by the District of Arizona to search the vehicle Moore-Jones drove to the Walmart. FBI Agents seized several items of evidence of the crime such as receipts from payments the victim made to Moore-Jones during the extortion scheme.

BACKGROUND ON ELECTRONIC DEVICES AND STORAGE

12. As used herein, a cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "land line" telephones. A cellular telephone usually includes a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, typically, cellular telephones also offer a broad range of capabilities. These capabilities include, but are not limited to: receiving and storing voice mail messages, storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and

accessing and downloading information from the Internet. Cellular telephones may also include global positioning systems ("GPS") technology for determining the location of the device.

13. Based upon my training and experience, it is common for extorters to maintain contact information in their cellular telephones of their co-conspirators and victims in order to communicate before, during, and after an extortion. In addition to making voice calls with their cellular phones, it is common for extorters to use text messaging service and messaging applications to contact victims and co-conspirators. Due to the technological nature of current cellular devices, a significant historical record of these communications are generally preserved on or in the memory of cellular phones. Additionally, current cellular telephones allow criminals to utilize map services to locate or navigate to various locations related to their crimes. This information is also preserved in the memory of the cellular phone.

14. As described above and in the Attached List, this application seeks permission to search and seize things that the media to be searched might contain, in whatever form they are stored. Digital and electronic files may be important to criminal investigations in several ways. In some cases, the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime. Further, the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in various forms of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime.

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device,

it can sometimes be recovered with forensic tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. Searching for the evidence described above may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in the Attached List, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the Federal Bureau of Investigation intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence from the seized items listed above.

17. The digital media to be search will be examined by one or more agents or law enforcement officers and technicians with specialized forensic training. In examining **subject telephone 1**, all searches will be limited to the device itself - the search will not involve contacting the service provider for the telephone to download information from the service provider to the device (e.g., voice mail or text messages that have not yet been delivered from the service provider to the device).

18. Because I seek a warrant to examine a device already in law enforcement's possession, the execution of the warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. Based upon the aforementioned facts, there is probable cause to believe that evidence of violations of Title 18, U.S.C. § 875(d); transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money, committed by Moore-Jones will be found in **subject telephone 1** described in Attachment A. I respectfully request the issuance of a warrant to search the media within **subject telephone 1** and seize the items described in Attachment B.

_____
KASSANDRA L. McKENZIE
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this _____ day of September, 2019.

_____
PATRICIA L. COHEN
United States Magistrate Court Judge
Eastern District of Missouri

ATTACHMENT A

DESCRIPTION OF ITEM TO BE SEARCHED

A pink iPhone Model A1897, IMEI 358632092187804.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records on the item described in Attachment A that relate to violations of Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money, including:
    a. lists of victims and/or people and related identifying information;
    b. photos and/or videos of sexual acts;
    c. electronic communications;
    d. phone logs, text messages, search history, travel history on the phone's GPS or location data;
    e. any information recording Moore-Jones and unidentified co-conspirator's schedules or travel to include any GPS data saved or stored on the device to be searched;
    f. Images or video regarding extortion or any related financial transactions.
2. All names, aliases, and numbers stored in the phones, including the number associated with **subject telephone 1** and any number directory stored in the memory of the phones that provides information regarding participants involved in violations of Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money.
3. Evidence of user attribution showing who used or owned the items to be searched at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
4. Records evidencing the use of the Internet to communicate via email social media websites, or other electronic means, regarding meeting locations with co-conspirators, customer purchases, shipments, financial transactions, including:
    a. records of Internet Protocol addresses used;
    b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.
6. All data files, including but not limited to, records and graphic representations, containing matter pertaining to the violation of Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money.
7. Graphic interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG) containing matter pertaining to the violation of Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money.
8. Electronic mail, chat logs, Internet Relay Chat (IRC) log files and electronic messages, concerning the violation Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money.
9. Log files and other records concerning dates and times of connection to the Internet and to websites pertaining to the violation Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money.
10. Any Instant Message conversations, chats, e-mails, text messages, or letters pertaining to the violation Title 18, U.S.C. § 875(d): transmitting in interstate commerce threats to injure the reputation of a person with the intent to extort money.